SECURITY INCIDENT SCREENSHOTS

1 Malware Detections (Event ID: 4688)

Time	User	src_ip	threat_type
04:19:14	alice	198.51.100.42	Rootkit Signature
05:45:14	david	172.16.0.3	Trojan Detected
05:48:14	bob	10.0.0.5	Trojan Detected
07:51:14	eve	10.0.0.5	Rootkit Signature
09:10:14	bob	172.16.0.3	Ransomware Behavior

2 Compromised Server: 172.16.0.3 (Event ID: 7000)

Time	User	Action	Status
04:41:14	alice	malware detected	Critical
05:18:14	charlie	login success	Suspicious
05:45:14	david	malware detected	Critical
07:45:14	charlie	malware detected	Critical
08:42:14	eve	file accessed	Investigate

SECURITY INCIDENT SCREENSHOTS (CONT.)

3 Suspicious Logins (Event ID: 4624/4625)

Time	User	src_ip	action
04:47:14	bob	10.0.0.5	login failed
05:04:14	bob	192.168.1.101	login success
07:02:14	alice	203.0.113.77	login failed
06:21:14	alice	203.0.113.77	login success
09:02:14	david	203.0.113.77	login failed

4 Anomalous Connections (Event ID: 5156)

Time	src_ip	dest_ip	protocol
06:13:14	10.0.0.5	203.0.113.77	HTTPS
07:44:14	203.0.113.77	10.0.0.5	SSH
08:20:14	192.168.1.101	172.16.0.3	RDP

5 Data Access Patterns (Event ID: 4663)

Time	User	src_ip	resource
06:10:14	david	203.0.113.77	file_server.docx
07:57:14	david	10.0.0.5	salaries.xlsx
09:10:14	bob	198.51.100.42	client_db.zip